regionernes sundheds-it

RAMMEDATABEHANDLERAFTALE

Mellem

Region Nordjylland og Aalborg Universitet

Denne databehandleraftale (herefter "Databehandleraftalen") vedrører databehandlerens forpligtelse til at efterleve EUROPA-PARLEMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) samt lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Denne Rammedatabehandleraftale er et bilag til "Samarbejdsaftale om fælles forskningsprojekt" mellem Aalborg Universitet og Region Nordjylland. Denne Rammedatabehandleraftale er et sæt vilkår, som er aftalt mellem Parterne i de tilfælde, hvor der er enighed om at der skal indgås en databehandleraftale. Vilkårene danner sammen med vilkårene i "Scope Of Work" de samlede vilkår for databehandlingen.

Databehandleraftalen er indgået mellem

Den Dataansvarlige (defineret i "Scope Of Work")
(herefter den *"Dataansvarlige"*)

og

Databehandler (defineret i Scope Of Work)
(herefter *"Databehandleren"*)

og er en del af aftalen "Samarbejdsaftale om fælles forskningsprojekt" og "Scope Of Work" (herefter "Hovedaftalen")

De oplysninger, som er omfattet af Databehandleraftalen, behandles (herefter bl.a. opbevares) på de i "Scope Of Work" nævnte adresse(r).

1. Databehandlerens ansvar

1.1. Databehandleren handler alene efter instruks fra den Dataansvarlige og alene i det omfang, det er nødvendigt for, at Databehandleren kan opfylde sine forpligtelser i henhold til Hovedaftalen og Databehandleraftalen.

Databehandleraftalen er således en del af den Dataansvarliges instruks til Databehandleren. Databehandleren må ikke behandle oplysninger omfattet af denne databehandleraftale til egne formål.

1.2. Databehandleraftalen frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

1.3. Hvis databehandleren er undergivet lovgivningen i et tredjeland, skal Databehandleren straks skriftligt orientere den Dataansvarlige, hvis den nævnte lovgivning forhindre Databehandleren i at efterleve databehandleraftalen og den dertil hørende instruks.

1.4. Hvis en Databehandler er underlagt national lovgivning, der hjemler behandling af personoplysninger, der strider mod Databehandleraftalen og den dertil hørende instruks, skal Dataansvarlige underrettes inden behandling påbegyndes, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

2. Databehandlerens opgave

2.1. Er defineret i Scope Of Work.

3. Tekniske og organisatoriske sikkerhedsforanstaltninger

3.1. Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med databeskyttelseslovgivningen.

Af bilag 1 fremgår minimumskrav til de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

3.2. Principperne og anbefalingerne i ISO 27001 med senere ændringer vil skulle anvendes som vejledende ramme ved overholdelse af kravene i nærværende databehandleraftale.

4. A. Databehandlerens brug af underdatabehandler

4.1. Databehandleren må ikke gøre brug af en Underdatabehandler til behandling af personoplysninger omfattet af denne databehandleraftale, medmindre dette fremgår af Scope Of Work og tilhørende bilag 2 (Databehandleraftalens bilag 2).

4.2. Anvendes en Underdatabehandler skal Databehandleren udlevere den indgåede databehandleraftale mellem Databehandleren og Underdatabehandleren på forespørgsel fra den Datasansvarlige. Databehandleren skal kunne dokumentere, at Underdatabehandleren er blevet instrueret, jf. bilag 1.

4.3. Databehandleren skal i sin aftale med Underdatabehandleren sikre sig, at Underdatabehandleren som minimum kan opfylde de databeskyttelsesforpligtelser, som Databehandleren har påtaget sig ved denne databehandleraftale for så vidt angår den behandling af personoplysninger, der varetages af Underdatabehandleren.

4.4. Databehandleren er ansvarlig for kontraktsmæssigheden og lovligheden af Underdatabehandlerens behandling af personoplysninger, herunder indgåelse af en databehandleraftale med mindst de forpligtelser, som Databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag. Det forhold, at Databehandleren indgår aftale med en Underdatabehandler, fritager ikke Databehandleren for pligten til at efterleve nærværende Databehandleraftale.

4.5. Ved ophør af en aftale med en Underdatabehandler om behandling af personoplysninger omfattet af denne Databehandleraftale, skal Databehandleren give den Dataansvarlige meddelelse herom. Databehandleren skal i den forbindelse sikre, at Underdatabehandleren sletter data behørigt i overensstemmelse med pkt. 9.

4.6. Databehandleren må endvidere ikke overføre eller tillade overførsel af personoplysninger til lande udenfor EU og det Europæiske Økonomiske Samarbejdsområde, medmindre de pågældende Underdatabehandlere fremgår af Databehandleraftalens bilag 2.

4.7. Såfremt den Dataansvarlige har givet Databehandleren en udtrykkelig tilladelse til en overførsel af personoplysninger til en Underdatabehandler i lande uden for EU og det Europæiske Økonomiske Samarbejdsområde, påhviler det Databehandleren at sikre, at data ikke overføres før, der foreligger et lovligt grundlag for overførsel af personoplysninger til de pågældende lande. Anvendes Underdatabehandler i lande uden for EU og det Europæiske Økonomiske Samarbejdsområde, skal dette fremgå i Databehandleraftalens bilag 2.

4.8. Databehandleren skal i sin aftale med Underdatabehandleren indføje den Dataansvarlige som begunstiget tredjemand i tilfælde af Databehandlerens konkurs, således at den Dataansvarlige kan indtræde i Databehandlerens rettigheder og gøre dem gældende over for Underdatabehandleren, f.eks. så den Dataansvarlige kan instruere Underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

4. B. Skift af Underdatabehandler i aftaleperioden

4.9. Databehandleren kan udpege en ny Underdatabehandler, såfremt den nye Underdatabehandler (1) overholder gældende love om databeskyttelse og (2) er

bundet af databehandleraftale eller en EU-model kontrakt eller tilsvarende og (3) har et sikkerhedsniveau, som er mindst det samme som den nuværende Underdatabehandler.

4.10. Databehandleren skal orientere den Dataansvarlige i tilfælde af, at der vælges ny Underdatabehandler. Orienteringen skal ske 3 måneder, inden den nye Underdatabehandler tages i anvendelse. Orienteringen skal sendes til systemejer eller projektansvarlig, jf. punkt 17.

4.11. Såfremt den Dataansvarlige ikke mener, at en af Databehandleren udpeget Underdatabehandler lever op til et eller flere af de ovennævnte krav under pkt. 4.9, nr. (1), (2) og (3), vil det blive betragtet som væsentlig misligholdelse, og der henvises til pkt. 13 om misligholdelse.

4.12. Den Dataansvarlige har på ethvert tidspunkt ret til fra Databehandleren at få udleveret en kopi af Databehandlerens aftale (flow down-aftaler) med de i bilag 2 pkt. 15 angivne Underdatabehandlere.

5. Overførsel af oplysninger til tredjelande eller internationale organisationer

5.1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret som Databehandleren er underlagt; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandling, medmindre de pågældende retlige krav forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

5.2. Uden den Dataansvarliges instruks eller godkendelse kan Databehandlerne - indenfor rammerne af Databehandleraftalen – derfor bl.a. ikke:

a. Videregive personoplysninger til en Dataansvarlig i et tredjeland eller i en international organisation,

b. Overlade behandlingen af personoplysninger til en Underdatabehandler i et tredjeland,

c. Lade oplysningerne behandle i en anden af Databehandlerens afdelinger, som er placeret i et tredjeland

5.3. Den Dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales bilag 2.

6. Ad hoc arbejdspladser

6.1. Såfremt Databehandleren foretager databehandling fra ad hoc arbejdspladser, skal Databehandleren sikre, at disse lever op til de sikkerhedsmæssige krav i

denne Databehandleraftale med bilag samt Datatilsynets IT-sikkerhedstekster herom.

6.2. Anvendes ad hoc arbejdspladser, skal dette nævnes i pkt. 15.

6.3. Databehandleren skal blandt andet opfylde og dokumentere følgende:

- Beskrivelse af anvendt krypteret forbindelse mellem ad hoc arbejdspladsen og Databehandlerens/dataansvarliges netværk.
- Anvendelse af 2-faktor-autentifikation.
- Databehandlerens interne instruks til egne medarbejdere vedrørende ad hoc arbejdspladser.

7. Tilsynsmyndigheder, audits og revisorerklæringer

7.1. Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige nødvendige oplysninger til, at denne kan påse forpligtelserne i henhold til denne aftale, herunder om de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger m.v. er truffet. Endvidere skal Databehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering.

7.2. I tilfælde af at den Dataansvarlige og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en fysisk inspektion (audit) af de foranstaltninger, som Databehandler foretager i medfør af Databehandleraftalen, forpligter Databehandleren sig til – med et rimeligt varsel – at stille tid og ressourcer i form af arbejdstid til rådighed herfor. Databehandleren forpligter sig på samme måde til at sikre, at sådanne audits også kan gennemføres hos dennes Underdatabehandlere af Databehandleren.

8. Underretning og assistance

8.1. Databehandleren forpligter sig til uden unødig forsinkelse og skriftligt at orientere den Dataansvarlige om afvigelser fra kravene i databehandleraftalen, f.eks.:

- ved enhver fravigelse fra givne instrukser
- ved enhver afvigelse fra det aftalte om tilgængelighed
- ved planlagte releases, opgraderinger, tests m.v.
- ved enhver mistanke om brud på fortroligheden, misbrug, fortabelse og forringelse af data mv.

8.2. Yderligere forpligter Databehandleren sig til uden unødig forsinkelse og skriftligt at orientere den Dataansvarlige om brud på persondatasikkerheden, f.eks.:

- ved enhver konstatering af misbrug, fortabelse og forringelse af data m.v.
- ved enhver hændelig eller uautoriseret videregivelse af eller adgang til personoplysninger behandlet efter denne Databehandleraftale.

En underretning om brud på persondatasikkerheden skal indeholdende følgende oplysninger:

- Karakteren af bruddet på datasikkerheden og, hvis det er muligt, hvem der er omfattet, antal berørte og antal berørte registreringer af personoplysninger.
- Beskrivelse af de sandsynlige konsekvenser, der er af bruddet.
- Beskrivelse af de foranstaltninger, Databehandleren har truffet eller foreslået truffet for at håndtere databruddet, og hvad der kan gøres for at begrænse dets mulige skadevirkninger.

Når Region Nordjylland er dataansvarlig:

Underretning om brud på persondatasikkerheden skal ske via denne side, under afsnittet *"Hvis der sker brud på informationssikkerheden"*: http://www.rn.dk/om-region-nordjylland/dine-rettigheder-naar-regionen-behandler-oplysninger-om-dig

Når Aalborg Universitet er dataansvarlig:

Underretning om brud på persondatasikkerheden skal ske ved kontakt til Databeskyttelsesrådgiveren på dpo@aau.dk.

8.3. Databehandleren skal uden unødig forsinkelse assistere den Dataansvarlige med håndteringen af enhver henvendelse fra en registreret for så vidt angår anmodning om udøvelse af den registreredes rettigheder, jf. kap. 3 i Databeskyttelsesforordningen, herunder f.eks.. indsigt, berigtigelse, blokering eller sletning, hvis de relevante personoplysninger behandles af Databehandleren.

8.4. Databehandleren skal assistere den Dataansvarlige med at overholde forpligtelser, der måtte påhvile den Dataansvarlige efter gældende ret, og hvor assistance er nødvendig for, at den Dataansvarlige kan overholde disse forpligtelser, herunder forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

9. Aftalens ikrafttræden og varighed

9.1. Databehandleraftalen træder i kraft ved underskrift fra alle parter.

9.2. Databehandleraftalen er gældende, så længe behandlingen består, og skal forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos Databehandleren og eventulle underdatabehandlere.

10. Håndtering af data efter aftalens ophør

10.1. Databehandleren og dennes eventuelle Underdatabehandlere forpligter sig til at tilbagelevere og/eller slette personoplysninger, når databehandlingen i henhold til Hovedaftalen ophører. Den Dataansvarlige skal oplyse Databehandleren om det tidspunkt, hvor databehandlingen skal ophøre. Det påhviler herefter Databehandleren at tilbagelevere og/eller slette personoplysningerne, samt at slette eksisterende kopier på det oplyste tidspunkt, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

10.2. Databehandleren er ansvarlig for at sletning af oplysningerne sker på en sådan måde, at det ikke er muligt at genskabe oplysningerne.

10.3. Når sletningen er foretaget, skal Databehandleren fremsende en skriftlig erklæring på, at data er slettet som aftalt.

10.4. Såfremt Databehandler eller dennes Underdatabehandlere i forbindelse med konkurs eller lignede ophører med at behandle personoplysninger for den Dataansvarlige, skal alle personoplysningerne straks leveres tilbage til den Dataansvarlige på en måde, der gør det muligt for den Dataansvarlige at anvende disse fremadrettet. Herefter er Databehandler, dennes konkursbo eller lignende forpligtet til effektivt at slette oplysningerne fra egne systemer i overensstemmelse med ovenstående.

11. Personoplysninger omfattet af denne aftale er fortrolige

11.1. Databehandleren skal sikre, og efter anmodning fra den Dataansvarlige kunne påvise, at de medarbejdere, underdatabehandlere, samarbejdspartnere, eksterne konsulenter og vikarer m.fl., der er autoriseret til at behandle de i aftalen omfattede personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

11.2. Det påhviler Databehandleren at informere medarbejdere, underdatabehandlere, samarbejdspartnere, eksterne konsulenter og vikarer m.fl. om tavshedspligten.

11.3. Databehandleren skal sikre, at adgangen til personoplysninger omfattet af denne Databehandleraftale er begrænset til de medarbejdere, for hvem det er nødvendigt at behandle personoplysninger for at kunne opfylde Databehandlerens forpligtelser over for den Dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.

11.4. Databehandlerens forpligtelser om tavshedspligt og fortrolighed gælder også efter Hovedaftalens ophør.

12. Overdragelse

12.1. Databehandleren må ikke overdrage sine rettigheder og forpligtelser i henhold til denne Databehandleraftale uden den Dataansvarliges forudgående samtykke.

13. Misligholdelse

13.1. Bestemmelserne i dette afsnit har forrang ift. Hovedaftalen, for så vidt angår behandlingen af personoplysninger.

13.2. Ved Databehandlerens misligholdelse af Databehandleraftalen er den Dataansvarlige berettiget til at gøre sædvanlige misligholdelsesbeføjelser gældende med de tilføjelser og præciseringer, som fremgår af bestemmelserne i dette afsnit.

13.3. Det betragtes som misligholdelse af Databehandleraftalen, såfremt Databehandler ikke overholder forpligtelserne i Databehandleraftalen, de til enhver tid gældende lovgivningsmæssige krav og kravene i Databehandleraftalens bilag 1.
Ved væsentlig misligholdelse – herunder ved gentagen misligholdelse, som ikke efter Dataansvarliges påkrav straks bringes til ophør – er den Dataansvarlige berettiget til at ophæve det konkrete samarbejde som defineret i Scope Of Work, såfremt Databehandleren ikke bringer misligholdelsen til ophør inden 14 dage fra Dataansvarliges meddelelse om, at misligholdelsen betragtes som væsentlig.

13.4. Den Dataansvarliges ophævelse af hovedaftalen og Databehandleraftalen indebærer ikke, at den Dataansvarlige giver afkald på sin ret til at kræve erstatning, hvis betingelserne herfor er opfyldt, jf. pkt. 13.7.

13.5. Såfremt den Dataansvarlige vælger ikke at ophæve det konkrete samarbejde som defineret i Scope Of Work i ét eller flere tilfælde, selvom den Dataansvarlige er berettiget hertil, medfører dette ikke, at den Dataansvarlige mister retten til at ophæve Hovedaftalen og Databehandleraftalen i andre tilfælde.

13.6. Ved ophævelse af det konkrete samarbejde som defineret i Scope of Work, er Databehandleren forpligtet til at levere databehandling i henhold til Scope Of Work og denne Databehandleraftale, indtil databehandlingen er sikret hos en anden databehandler. Databehandleren er ligeledes forpligtet til at levere relevant ophørsassistance til den Dataansvarlige, herunder i relation til eventuelle Underdatabehandlere, som Databehandleren måtte have overladt en del af databehandlingen til.

13.7. Databehandleren er erstatningsansvarlig i overensstemmelse med dansk rets almindelige regler i tilfælde af misligholdelse af Databehandleraftalen.

13.8. Såfremt den Dataansvarlige af tredjemand gøres erstatningsansvarlig for Databehandlerens og/eller eventuelle Underdatabehandleres forsætlige eller groft uagtsomme overtrædelse af Databehandleraftalen, herunder Databehandleraftalens bilag, og/eller gældende lovgivning vedrørende databeskyttelse, skal Databehandleren holde den Dataansvarlige skadesløs for alle omkostninger, gebyrer,

erstatningsbeløb, udgifter eller tab, som den Dataansvarlige har afholdt eller pådraget sig som følgende heraf.

14. Lovvalg og værneting

14.1. Bestemmelserne i dette afsnit finder ikke anvendelse, såfremt lovvalg og værneting er særskilt reguleret i Hovedaftalen.

14.2. Denne Databehandleraftale inklusiv ethvert spørgsmål om Databehandleraftalens gyldighed er undergivet dansk ret.

14.3. *Forhandling*
Såfremt der opstår en uoverensstemmelse mellem Parterne i forbindelse med Databehandleraftalen, skal Parterne med en positiv, samarbejdende og ansvarlig holdning sørge for at indlede forhandlinger med henblik på at løse tvisten.

14.4. *Domstolsbehandling*
Hvis enighed ikke kan opnås via forhandling eller på anden vis, skal tvisten løses ved de danske domstole ved den Dataansvarliges hjemting.

15. Ændringer til punkterne 1-14

15.1. Hvis det er tvingende nødvendigt at ændre punkterne 1-14, skal ændringerne beskrives her.

15.2. Den Dataansvarlige godkender Databehandlerens brug af ad hoc arbejdspladser, forudsat at Databehandleren benytter VPN og 2-faktor log in.

16. Bilag

Bilag 1: Databehandlerinstruks
Bilag 2: Underdatabehandler til Databehandleren

17. Underskrifter

På vegne af Region Nordjylland:

Navn: Søren Pihlkjær Hjortshøj
Stilling: Forskningschef

Dato: 3/7 - 2019

Underskrift:

På vegne af Aalborg Universitet:

Navn: Lars Hvilsted Rasmussen
Stilling: Dekan for det Sundhedsvidenskabelige fakultet

Dato: 27.06.2019

Underskrift:

Navn: Nina Schjoldager
Stilling: Kontraktchef

Dato: 27/6-2019

Underskrift: Nina Schjoldager

Bilag 1

DATABEHANDLERINSTRUKS

Ad. 1. Databehandlerens ansvar

1.1 Databehandling omfattet af Databehandleraftalen skal ske i overensstemmelse med denne instruks.

Ad. 3. Tekniske og organisatoriske sikkerhedsforanstaltninger

3.1 Databehandleren skal på et generelt niveau træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af personoplysninger omfattet af Databehandleraftalen.

3.1.1 Såfremt mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger er nødvendige for at sikre efterlevelse af Databehandleraftalens punkt 3, skal sådanne foranstaltninger altid træffes.

3.2 Risici for sikkerhed

3.2.1 Databehandleren skal tage de nødvendige skridt til at identificere enhver risiko for tilgængeligheden, fortroligheden, og/eller integriteten af alle personoplysninger omfattet af Databehandleraftalen.

3.2.2 Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal evaluere og forbedre effektiviteten af sådanne forholdsregler, når det er nødvendigt.

3.2.3 Databehandleren skal dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau.

Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

a. Pseudonymisering og kryptering af personoplysninger
b. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og - tjenester
c. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed

3.2.4 Databehandleren skal have formelle procedurer for håndtering af sikkerhedshændelser.

3.3 Autorisation og adgangskontrol

3.3.1 Såfremt Databehandleren bruger den eneste kopi af data, der findes, skal autorisationer angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.

3.3.2 Kun de personer som autoriseres dertil, må have adgang til de personoplysninger, der behandles i henhold til Databehandleraftalen.

3.3.3 Databehandleren skal kunne dokumentere hvilke medarbejder der har autorisation til at tilgå personoplysninger, der behandles i henhold til Databehandleraftalen.

3.3.4 Autoriserede personer skal kunne fremvise billed-id ved on-site databehandling hos Dataansvarlig.

3.3.5 Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har brug for.

3.3.6 Der må endvidere autoriseres personer, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

3.3.7 Den autoriserede bruger udstyres med en personlig brugeridentifikation og et personligt password, der skal anvendes hver gang, brugerne får adgang til databehandlingen. Passwords skal skiftes minimum hvert halve år. Passwords skal have en tilstrækkelig længde og kompleksitet. Som udgangspunkt anvendes 2 faktor-autentifikation ved adgang til systemer med følsomme personoplysninger via internettet eller andet usikkert netværk. Autentifikationsmetoden kan f.eks. være Nem-id, SMS-token, Rfid eller lignende.

3.3.8 Databehandleren skal træffe foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til de personoplysninger, som den pågældende er autoriseret til.

3.3.9 Databehandleren skal have rimelige restriktioner for fysisk adgang. Områder hvor der sker behandling af personoplysninger i henhold til Hovedaftalen, skal være effektivt adskilt fra områder, hvortil der er generel adgang.

3.3.10 Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

3.3.11 Databehandleren skal uden unødig forsinkelse inddrage autorisationer og adgange for brugere, der efter en konkret vurdering ikke længere bør have disse.

3.4 Uddannelse og instruktion

3.4.1 Databehandleren skal sørge for, at dennes medarbejdere modtager den tilstrækkelige uddannelse og instruktioner for at sikre, at personoplysninger behandles i overensstemmelse med relevant lovgivning og vilkår i databehandleraftalen.

3.5 Kontrol med afviste adgangsforsøg og logning

3.5.1 Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret højst 3 på hinanden følgende afviste adgangsforsøg med samme brugeridentifikation, skal der blokeres for yderligere forsøg fra denne brugeridentifikation. Adgangen åbnes først, når årsagen til afviste adgangsforsøg er klarlagt.

3.5.2 Der skal foretages maskinel registrering (logning) ved behandling af personoplysninger omfattet af art. 9 og 10 i den generelle forordning om databeskyttelse. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger og type af anvendelse, fsva. opretteIse og sletning af filer. Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode, af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

3.6 Inddatamateriale

3.6.1 Inddatamateriale må kun anvendes af personer, som er beskæftiget med inddateringen. Inddatamateriale skal opbevares på en sådan måde, at uvedkommende ikke kan gøre sig bekendt med de personoplysninger, der er indeholdt heri.

3.6.2 Når det ikke længere er nødvendigt at bevare inddatamaterialet, skal Databehandleren slette eller tilintetgøre inddatamaterialet. Fremgangsmåden herfor skal ske efter best practice.

3.6.3 Bestemmelsen vedrørende sletning eller tilintetgørelse gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser i henhold til anden lovgivning, eller hvis journaliseret materiale behandles efter de almindelige arkivbestemmelser om bevaring, herunder aflevering af arkivalier til Rigsarkivet.

3.7 Uddatamateriale

3.7.1 Uddatamateriale er omfattet af samme instrukser som inddatamateriale med følgende tilføjelse:

3.7.2 Uddata må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages, samt i forbindelse med revision, teknisk vedligeholdelse, driftsovervågning og fejlretning mv.

3.8 Mobile lagringsmedier

3.8.1 Mobile lagringsmedier med personoplysninger skal være mærket, og skal opbevares med en tilstrækkelig stærk kryptering og under opsyn eller under lås, når de ikke benyttes.

3.8.2 Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver.

3.8.3 Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af udtagelige mobile lagringsmedier.

3.8.4 I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov. Dette skal ske efter best practice.

3.9 Sikkerhedskopier

3.9.1 Der gælder de samme retningslinjer for sikkerhedskopier som for al anden behandling af personoplysninger i medfør af denne aftale.

3.9.2 Databehandleren skal sikre, at systemer og personoplysninger sikkerhedskopieres regelmæssigt.

3.9.3 Sikkerhedskopier skal opbevares adskilt fra serveren i et ikke tilstødende rum for at sikre, at disse ikke går tabt f.eks. som følge af brand eller oversvømmelse. Opbevaring af sikkerhedskopier skal altid ske på betryggende vis så de ikke fortabes.

3.9.4 Databehandleren skal regelmæssigt kontrollere, at sikkerhedskopier er læsbare. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af et systems tekniske setup.

3.10 Opdateringer og ændringer

3.10.1 Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

3.10.2 Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse eller ledelsesopfølgning med henblik på at sikre, at ingen enkeltpersoner kan implementere en ændring alene.

3.11 Driftsafbrydelser

3.11.1 Databehandleren skal have dokumenterede beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser.

3.12 Bortskaffelse af udstyr

3.12.1 Databehandleren skal have formelle processer i overensstemmelse med best practice og Dataansvarliges krav med henblik på at sikre, at der sker effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

3.12.2 Ved bortskaffelse af udstyr skal Databehandleren dokumentere fremgangsmåden herfor, og kunne forevise denne dokumentation efter anmodning herom.

3.13 Tilsyn

3.13.1 Databehandleren skal føre og dokumentere et tilsyn med Databehandlerens organisations overholdelse af lovkrav, politikker, procedurer og denne Databehandleraftale med bilag.

Ad. 6. Ad hoc arbejdspladser

6.1 Databehandleren må ikke foretage databehandling fra ad hoc arbejdspladser (fjernarbejdspladser eller hjemmearbejdspladser), medmindre Databehandleraftalens punkt 15 indeholder en beskrivelse heraf.

6.1.1 Den Dataansvarlige skal godkende brug af ad hoc arbejdspladser.

Der henvises til Databehandleraftalens punkt 15.2.

6.1.2 Eksterne kommunikationsforbindelser skal leve op til Datatilsynets it-sikkerhedstekst ST1.

6.1.3 Der skal anvendes 2-faktor-autentifikation. Autentifikationsmetoden kan f.eks. være Nem-id, SMS-token, Rfid eller lignende.

6.1.4 Der må kun etableres eksterne IT-kommunikationsforbindelser, hvis der efter godkendelse og efter nærmere aftale herom træffes foranstaltninger til at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.